Botnet Detection using Traffic Analysis and Defenses

Shreyash Mulik, Aishwarya Patil
shreyash.mulik@adypu.edu.in, aishwarya.patil@adypu.edu.in
B-Tech CTIS
Ajeenkya DY Patil University, Pune, India

Abstract- The abstinence progression of Botnet malware made it acutely serve to detect. Even though it can be just considered as a tool, now attackers who are not at all more stimulated to just attract media attention by infecting a huge number of computers on the network. They are used to allocate direction to the Bots for malicious actions such as distributed denial-of-service (DDOS) occurrences, junk and phishing. Huge number of the prevalent Botnet detection techniques only on particular Botnet command and control and structures and can develop into inflated as Botnets change their construction and C&C techniques. A Bot is a type of malware that allows an attacker to take control of infected machine. The Botnet is a network of bots. A Bot infected machine is often called as zombie and cybercriminals who control these bots are called Botherders. Bots are often spread themselves across internet by searching for unsafe machines to expand. The way the bots are controlled depends upon architecture of botnet Command and Control mechanism which may be based on Internet Relay Chat or HTTP or Peer to Peer. Botnet is widely used to carry out malicious activities like Distributed Denial of Service (DDoS) attacks, sending spam mails and click frauds. In recent years, botnet-based attacks have become more sophisticated and can bypass all security safeguards.

Index Terms- Traffic behavior analysis, Botnet, Cyber security, IRC, C&C, DDOS

1) INTRODUCTION

A "botnet" is defined as a network of infected hosts (Bots) which are running software robots and are being supervised by a human (botherder), through one or more than one controllers (botmasters). The botmaster's intercommunication with its bots is called Command and Control (C&C) traffic. Botnets root in purposed security threat. A Bot is a type of malware which consent third party to take authority of machine that is infected. A Bot infected machine is often called as zombie and attackers or third party who supervise these bots are called Botherders or Botmasters. Bots usually transmit themselves across the internet in exploration of vulnerable machines to enlarge. The way the bots are audit depends upon architecture of botnet Command and Control (C&C) mechanism which may be based on Internet Relay Chat (IRC) or HTTP or Peer to Peer (P2P). Botnet is worn in malicious activities like Distributed Denial of Service (DDOS) attacks, sending spam mails and click frauds.

Botnet detection methods take measure abundantly speaking supported either fitting of a protea to gather larva binaries or developing intrusion detection system. The intrusion detection system(IDS) establish botnet traffic by conclusion network and system logs. It can be based on incongruity behavior or signature or DNS. The Net flow analyzer is boundless tool for informer work botnet anomaly primarily based detection. The Snort, Suricata, Ntop, Bothunter square measure other tools that take measure supported signatures of botnet. The DNS primarily based botnet traffic is supervised by Wire shark. The BotMiner tool profit bunch algorithmic rule to observe botnet. Zeus toolkit is widespread in the thick of hacker's community for analysis of botnet internals.

When associate degree assaulter passes the directions on to bots, IRC is mostly used as some way of communications. IRC is a talking system that exchanges the client's messages for text data on the TCP/IP protocol through servers. Some C&C servers are designed in such some way that it immediately replies to bot's initial request.

• Waiting: when connection to network, larva waits for command from C&C server. During this section little traffic is found between larva and its master.

• Executing: Once the larva received command from its master, it starts capital punishment it. After execution it sends result to larva master via C&C network. Typical commands are: scanning for brand
new victims, causation spam, and causation DOS flood.

There are 2 main botnet topologies:

Centralized and peer to look (P2P). In centralized botnets, IRC continues to be pre dominant protocol of C&C channel. Currently this trend is decreasing and new bots accompany hypertext transfer protocol for his or her C&C channel. The main disadvantage of centralized botnets is single purpose failure. If centralized entity is removed the whole network is unusable. But, fashionable botnets overcome this downside by mistreatment fast-flux DNS techniques.

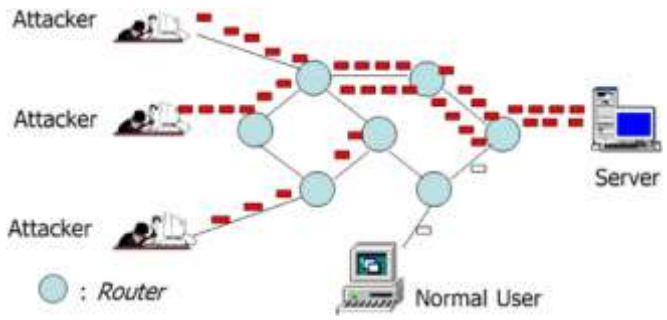
In quick flux DNS techniques, it's terribly tough to trace central entity. The compromised hosts are used as proxies to cover identities of true C&C servers. These hosts perpetually alternate DNS configuration to resolve one hostname with multiple information science addresses. Popular examples of IRC bots are Agobot, Spybot, and Sdbot.

2) Literature Analysis

Botnet in DDOS Attacks: Trends and Challenges

Nazrul Hoque, presented comprehensive overview of DDOS attack. The paper also contains detail discussion of botnet architecture; tools developed using botnet architectures to perform DDOS attack. This paper also summarized important issues and research challenges. In context to DDOS, there are two categories of botnet, DDOS attack using stationary botnet and DDOS attack using mobile botnet. There are four reasons behind using botnet for performing DDOS attack:

1. Large number of zombie nodes allows generation of powerful flood attacks quickly
2. Difficulty to identify the main attacker
3. Facility to benefit protocols to detour security mechanisms



4. Difficulty in real time detection Botnet based DDOS attack is basically launched using three basic models: Agent handler model, web-based model and IRC based model. It summarizes all existing stationary and mobile botnets. Botnet detection methods are typically classified into two categories: analysis of passive traffic and traffic generated by honey net. This paper raises issues in existing DDOS detection methods: Existing detection method is capable to detect low .The performance of most method depend on network conditions and parameters.

Botnet Detection Techniques:

Review, Future Trends, and Issues Ahmad Karim, presents a comprehensive review of the latest state-of-the-art techniques for botnet detection and figures out the trends of previous and current research. The author also discusses future direction of botnet detection techniques. Researchers have developed many architectures and botnet detection taxonomies. The honey nets are used to collect information about bots for analysis such as finding botnet characteristics, finding tools used behind attack and motivation behind the attack. Intrusion detection system is a software application or hardware to monitor 6 system services for malicious activities or policy violations and accordingly generate reports. This paper also explains future trends of botnets:

• **Social botnets**:- Botmasters now capture a huge audience while remaining hidden from it. They try to exploit social media sites such as Facebook and Twitter. Botnet Butterfly is one of the profitable botnets which damaged 12 million PCs worldwide.

• **Mobile botnets**: Mobile botnets are a serious threat to smart phones. Hacker's objective is to perform illegal phone calls, sending emails, illegal photo access. The most popular mobile botnets are Dream droid, Zeus and Tigerbot.

• **Botnets to Botclouds**: Dark clouds are controlled by cyber criminals which are silently infect networks. The author also put light on open issues in botnet detection techniques.

• Most of techniques are not accurately measure the size of the botnet.

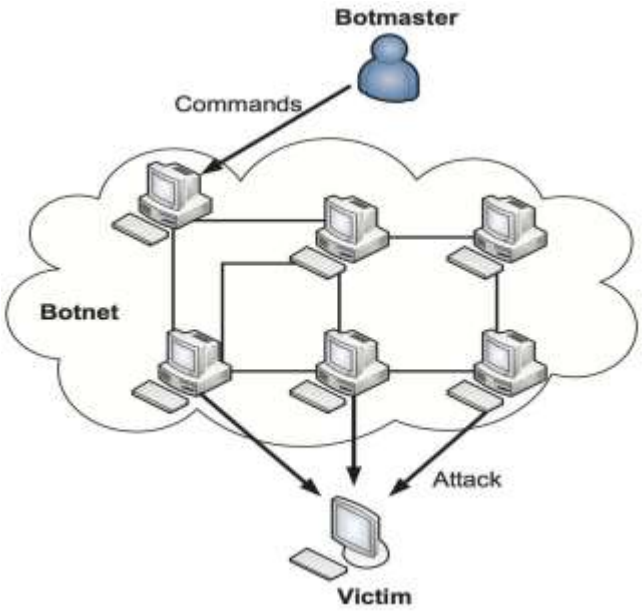
• Researchers face difficulty in obtaining real trace. They also find difficulties in comparing their result with previously published benchmark because datasets to full extent are not easily accessible to research domain.

Detecting Botnet by Anomalous Traffic Chia-Mei Chen, explained anomaly score-based botnet detection to identify the botnet activities. The author uses the similarity measurement and the periodic characteristics of botnets to employs two-level correlation relating the set of hosts with same anomaly behaviors. This method can differentiate the malicious network traffic generated by infected hosts (bots) from that by normal IRC clients. This method is also applicable for small size of botnets. The author observer IRC traffic within an organization network domain and identifies the infected host and suspicious C&C server. This method identifies infected machine even if it generates small traffic. It is also useful to detect C&C server. The author proposed method performs following steps:

1. IRC bot traffic collection at organization gateway.
2. The attributes of network traffic are extracted from packet header and payload; it is called as feature extraction. Here the following flow attributes are selected for further analysis: Source IP, Destination Ip, Source port, Destination port, Timestamp, Payload.
3. **Correlation Traffic:** It employs the homogeneous response and the group activity patterns to identify such anomalous machines. Normal machines respond randomly whereas infected bot machines respond at some regular interval and exhibit similar response pattern. The author proposed two levels of correlation.
4. **Anomaly Scoring:** Among different group flows, the group flow occurring in a shorter time span is more likely to be a botnet. If anomaly scoring exceeds certain threshold it generates alerts to administrator.

3) Command and control

A botmasters communication with the botnet is carried out via C&C. The C&C is that the main feature that distinguishes botnets from alternative malwares. It permits the botmasters to speak with the botnet and provides commands. On paper, the botmaster will command the botnet to try and do any task including; playing DDOS attacks, spamming, spying, fraud etc. To avoid detection, botnet designers tend to use wide used protocols for his or her C&C. Most botnets use IRC commands for his or her C&C communication. However, some botnets use the communications protocol, POP3 or P2P protocols for their C&C communication. Fresh rising styles of botnets use SMS, MMS, or on-line social networks for C&C communication. The IRC, communications protocol and POP3 botnets square measure sometimes centralized within the sense that their C&C channels rely on specific servers and if they're disabled, botnet can stop to exist.



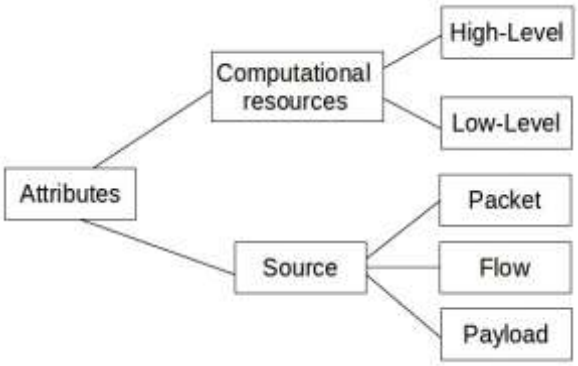
Behavior-Most botnets run in four phases. A lump transition from a clear host to a zombie host, and responding to its botmaster's supervision, goes through four steps. First, the initial infection starts once botnet nodes scan the network searching for vulnerabilities. They scan for backdoors, acknowledged buffer overflows, acknowledged vulnerable network administrator tools. They will run brute force word scanning for a few services (e.g. SQL servers, NetBIOS shares ... etc.) . Second, the secondary injection starts once vulnerability is exploited and therefore the victim host downloads and runs the bot's computer code. Then, the larva establishes an association to the botnet's C&C server, and starts to regulate the host (e.g. disable anti-virus, modification NetBIOS shares ... etc.). Finally, the malicious activities begin once the larva starts to act on botmaster's commands (e.g. run DOS attack, send SPAM...etc.) then the botnet maintains and upgrades itself periodically .In the case of P2P botnet, the primary 2 steps area unit similar to different botnets. Once the initial infection and injection, the P2P botnet uses AN initial peer list to contact the initial peers. Once it finds a live peer, part one starts wherever botnet updates its peer list and transfer any obtainable updates. Subsequently the node goes to part 2 once it starts its malicious activities. The aforesaid P2P botnet behavior is predicated on the STORM malware behavior. Different P2P malwares ought to -to some extend have similar behavior.

4) Features

The term attributes or features is usually related to data mining or machine learning process. However, for the purpose of our study, features are defined as certain characteristics of a set of data that can be obtained from network traffic captures. The analysis of network traffic features are the bases for network-based IDS.

There are two attributes classifications, one related to the computational resources needed to be obtained and the other one to the network traffic source. In the first classification, there are two cases: low-level features that can be acquired from raw traffic captures (as IP headers, or protocol) and high-level features that are the results of the traffic capture processing. For instance: Bytes per packet, packets per second, etc. These features might be obtained from low-level attributes.

The second classification mentioned, has three possibilities: packet, flow and payload features. These are obtained from packet headers, the information of network connections and packet payload (application layer) respectively. To clarify this classification, we present a diagram in Fig.



5) C & C Traffic

Based on few IRC attributes, Mazzariello modelled IRC user behavior. The author's target was to separate human user generated traffic from machine-driven IRC traffic exploitation language complexness, vocabulary and response times. Support Vector Machine (SVM) and J48 decision trees were employed in the experiment. Though the experiment was successful, it absolutely was not clear if this was due to the formula or the dataset used.

Stray et al used filters in pipeline manner to separate botnet traffic. The filtered botnet traffic flows are classified into IRC and non-IRC flows. Then, the formula appearance for relationships between these flows within the correlation stage. Finally, the Topological Analysis stage takes place in 3 steps. First, trying to find common endpoints by examining clusters scientific discipline addresses. Second, correlating traffic clusters by locating traffic in different flows that share an equivalent terminus. Third, flows are examined to find out that one is between the botmaster and also the endpoint.

Bot generated Traffic-Binkley et al. tried to discover IRC botnets supported traffic anomaly. They thought of associate degree IRC channel to be malicious if most of its host's square measure performing arts communications protocol SYN scanning. They collected 3 tuples for his or her analysis;

(1) communications protocol SYN scanner to see varieties of scanning on the network,

(2) IRC channel list to see IRC channel name and IRC hosts within the channel,

(3) IRC node list to see any informatics address that belongs to any IRC channel. exploitation these tuples, they were ready to generate reports of malicious channels, type IRC channels by most variety of messages, analyze host statistics of IRC channels, record IRC servers, ...etc. This formula is not signature-based and may work with unknown IRC botnets; however, it cannot discover encrypted botnets.

Akiyama et al. Advised that bots of identical botnet have regularities in relationship, response and synchronization and used these measures for botnet detection. Since all bots take commands from the botmaster, there's a one-to-many relationship -between the bots and their botmaster- even though there's no direct association over one layer. Additionally, once bots receive command from the botmaster, they respond mechanically and while not mistakes. This is often terribly completely different from human responses whereas chatting. What is more, once bots receive a command, they take identical action nearly at the same time. As an example, once the botmaster sends commands for DDOS attack; all collaborating bots begin the attack at identical time. This synchronization is employed asa detection metric lives. This detection technique may falsely establish high-demand legitimate nodes as botmasters.

5.1) DNS Traffic

Botmaster use DNS rallying to create their botnets invisible and moveable. Choi et al planned botnet detection mechanism by observance their DNS traffic. In keeping with the authors, bots use DNS queries either to attach or to migrate to a different C&C server. The DNS traffic has a distinctive feature that they outline as cluster activity. Bots is detected by exploitation the cluster activity property of botnet DNS traffic whereas bots square measure connecting to their server or migrating to a different server. There square measure 3 factors that facilitate in distinctive botnet DNS queries from legitimate DNS queries [20]; (1) queries to C&C servers come solely from botnet members (fixed information processing address area size),

(2) Botnet members migrate and act at constant time that ends up in temporary and synchronic DNS queries

(3) Botnets sometimes use DDNS for C&C servers. For a larva master to stay its bot hidden and moveable, it depends on DNS to rally infected hosts. In botnets, DNS queries will seem for several reasons.

They seem throughout rallying method once infection, throughout malicious activities like spam or DOS attacks, throughout C&C server migration, throughout C&C server information processing address amendment, or once C&C server or network link failure. Supported the

said 5 things of DNS question utilized in botnets, the authors have developed a Botnet DNS Q Detection algorithms, that distinguishes the botnet. This formula starts by building a info for DNS queries comprised of the supply information processing address, name and timestamp. Then, they cluster DNS question knowledge exploitation the name and timestamp field. After that, they take away redundant DNS queries. Finally, botnet DNS queries square measure detected employing a numerically computed some similarity factor. This formula cannot sight botnets migrating to a different C&C server.

Bot Master Trackback Detection-Most of the analysis on botnets focuses on detection and removal of C&C servers and bots in an exceedingly network. Detection of botmasters isn't addressed as actually because it is a tougher task. Botmasters don't got to stay on-line for long periods of your time. As presently as they furnish their command(s), they'll go offline and leave the hard work to their bots need to be disbursed in period. Moreover, botmaster sometimes hook up with their bots via stepping stones in order to cover themselves. Botmaster's C&C traffic is always low-volume and botmaster could hide it even a lot of using encoding. D. Ramsbrock et al projected a unique period watermarking botmaster trace back technique that's resilient to encoding and stepping stones.

They assumed that their tracer is up to the mark of a larva that is capable of responding to the botmaster. Their approach depends on this larva node injecting watermark once it responses to the botmaster. The watermarking is applied as follows:

(1) Random packet pairs square measure elect.

(2) The length of those packets square measure adjusted by artefact during a approach that the length distinction in every packet try falls into predefined vary.

(3) For encrypted botnet traffic, they developed a hybrid length-timing watermarking technique in which the watermarking packet got to be sent at specific time. For his or her hybrid length-timing watermarking method to figure, the belief that network interference is limited and information of the provision time of every watermarking packet should hold.

6) Detection Using Virtual machines

A detection technique that is supported virtual machine analysis of program executions. This system is predicated on the belief that bots ought to have 3 main features;

(1) The larva program starts mechanically while not user intervention,

(2) The larva should begin C&C communication,

(3) The larva should launch Associate in nursing attack. The BotTracer begins by beginning a virtual machine (on constant host) that has identical image of the host system once it starts.

This virtual machine will have all auto start processes on the first host however it will be free from any human interaction. Then, the BotTracer can monitor of these processes' automatic communications to notice C&C communications. Finally, BotTracer monitors the processes -that initiated suspected C&C communication- for all system-level activities and traffic patterns. Therefore, once a larva starts malicious activity, it'll be detected. This is often a time period technique that is capable of police investigation unknown bots no matter their protocol, with low false positive rate, notwithstanding the C&C traffic is encrypted. However, BotTracer has high computational demand thence virtual machine can degrade the user performance. The BotTracer won't defend against zero-day attacks wherever the larva keeps inactive waiting for a selected date and time. Moreover, for many bots that check for virtual machine presence, the BotTracer won't work.

Examples of Botnet Detection System-Botnet detection system mostly use one or more detection system. For example, signature could be used by detection system, C&C and botnet generated traffic to detect botnets. Therefore, it's not possible to place these detection systems below one classification.

this is often associate degree IRC-based botnet detection system that uses IRC channel names for detection. It monitors the network traffic for suspicious IRC channel names. Rishi starts by filtering all communications protocol packets containing IRC-related headers. These packets are identified by any of those keywords; NICK, JOIN, USER, QUIT and MODE. Then the subsequent info is extracted from the captured packets; connection time, supply port and scientific discipline address, destination port and scientific discipline address, IRC channel and IRC nickname. After that, nicknames are passed to the analyzer wherever they're scored. Higher scores replicate higher chance of botnet connections. Connections with scores on top of a predetermined threshold are marked as suspicious and a warning email is generated and sent to the network administrator.

BotHunter: this can be a botnet detection system that is supported a predefined botnet infection lifecycle. This technique works in real time and may find bots in spite of the network protocol or C&C structure as long because the botnet's behavior follows a predefined infection cycle dialog model (i.e. target scanning, infection exploitation, botnet binary downloading, botnet code execution, C&C communication and outward-bound scanning). BotHunter is comprised of 3 engines; applied mathematics scan Anomaly Detection Engine (SCADE), applied mathematics payload Anomaly Detection Engine (SLADE) and Signature Engine. SCADE is chargeable for the detection of incoming and outward-bound scan activities. SLADE detects abnormalities in byte-distribution payloads. The signature engine

is capable of detective work dialog warnings from a predefined botnet infection warning model. Furthermore, Bothunter uses a correlate to judge all messages (dialogs) from the anomaly detection engines (SCADE and SLADE).

BotSniffer:

this is often a botnet detection system that is supported traffic anomaly in native space Networks (LANs.). It's supported the belief that all the bots reply to a command in crowds and in the same manner. It's for similarities in botnet's traffic spatial-temporal correlations. The BotSniffer formula is comprised of 2 main blocks, monitor engine and correlation engine. The monitor engine is formed of 2 parts;

(1) Pre-processing: to scale back traffic volume victimization filters and whitelists.

(2) C&C-like protocol matchmaker: to gather suspicious IRC and hypertext transfer protocol traffic victimization port independent protocol matcher.

BotMiner:

this can be a botnet detection system that's supported a framework made from 3 main phases; watching, clustering, and correlating.

First, within the watching section, 2 watching engines -namely C&C communication traffic engine (Cplane), and activity engine (A-plane)- area unit used. Each engine keeps logs of its traffic analysis. The C-plane monitor each communications protocol and UDP flows to work out World Health Organization is lecturing whom. The A-plane monitor's network activities to work out World Health Organization are doing what (e.g. scan, spam) by detection abnormally-high scan rates or weighted failing association rate. Second, within the clump section, the C-plane clump is performed by looking for clusters of hosts that share same communication patterns. These clusters area unit used by calculating four random variables, namely; range of flows per hour, range of packets per hour, average range of bytes per packet and average range of bytes per second.

6.1) Defence and Post-Detection Reaction:

To , once a botnet is detected, it has to be half-tracked and brought down. First, a duplicate of the larva needs to be analyzed to grasp the larva behavior. To get a duplicate of the larva, the instrument has to use ways similar to honeypots. After that, the bots code has to be studied to search out ; however, the communication is finished within the botnet, however will new members be part of the botnet, and notice the whereabouts of the botmaster. Finally, the supply of the larva is brought down (physically) by the authorities. Very few papers planned post-detection procedures against botnet. Vogt et al advised that super botnets should be examined by the analysis community, so that defences against this threat are often developed proactively. They discovered some weak aspects of C&C mechanism that area unit exhibited by ancient botnet and counsel defenders to focus on these weaknesses. They finished that there are a unit 5 goal that defenders might take into account to create a psychoanalytic process against botnets:

1) Find or determine the person: At the time the adversary problems commands through the botnets' C&C, it becomes susceptible to detection.

2) Reveal all the infected machines: If bots area unit pooling for botnets' commands from a well-known location, this polling activity will be wont to reveal infected machines.

3) Command the botnet: Once the defender is acquainted with the botnets' commands, (s) he will send a command to the botnet to shut it down.

4) Disable the botnet: The botnet may by paralyzed by closing down its C&C channel.

5) Disrupt Botnet Commands: By ever-changing few bits in the adversary's commands is ample to disrupt adversary's management of the botnet.

7) CONCLUSION

Despite the very fact that our data concerning botnets is incomplete; botnets square measure one in all the foremost serious threats to network security. this survey was conducted to raised understand botnets and is an effort to arrange the enormous background accessible during this space to assist researchers who square measure beginning during this space. in this research, we have a tendency to explained botnets c&c communication, infection behaviors and models. we classified botnets -based on their underlying c&c protocol- to irc, http, pop3, and p2p botnets. as a new rising malware, social and mobile botnets' threats and potential were mentioned during this survey. as mobile phones with networking capabilities became additional affordable, the threat of mobile botnets have redoubled. mobile botnets might unfold through sms or mms services. their result can be terribly damaging because the security measures against mobile botnets might not are designed for mobile device. furthermore, botnet detection strategies square measure surveyed in detail. detection strategies are classified into three categories. first, behavior-based detection wherever botnets square measure detected using; c&c traffic behavior, larva generated traffic behavior, or dns traffic behavior. second, botmaster trace back detection is delineated. then, a virtual machine detection methodology is explained. finally, samples of botnets detection systems were explained (i.e. rishi, Bothunter, BotSniffer and BotMiner). the survey is ended with the botnets defense measures that should be taken when detection a botnet.

8) REFERENCES

[1] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet," *Computer Networks*, June 2012.

[2] I. C. Lin and C. H. Peng, "A survey of botnet architecture and botnet detectection techniques," *International Journal of Network Security*, vol. 0, pp. 81– 89, Mar. 2014.

[3] http://www.techtimes.com/articles/21714/20141208/ddos-attackcripples-sony-psn-while-microsoft-deals-with-xbox-live-woes.htm,

[4] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

[5] http://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar/

[6] Phatak, D., Sherman, A. T., Joshi, N., Sonawane, B., Relan, V. G., & Dawalbhakta, A. (2013). Spread Identity: A new dynamic address remapping mechanism for anonymity and DDoS defense. *Journal of Computer Security, 21 (2), 233-281.*

[7] Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R. W. (2005). *Inside Network Perimeter Security (Inside)*. Sams.

[8] J. Woodbridge, H. S. Anderson, A. Ahuja, and D. Grant, "Predicting domain generation algorithms with long short-term memory networks," *arXiv preprint arXiv:1611.00791*, 2016.

[9] P. Lison and V. Mavroeidis, "Automatic detection of malware-generated domains with recurrent neural models," *arXiv preprint arXiv:1709.07102*, 2017.

[10] H. Mac, D. Tran, V. Tong, L. G. Nguyen, and H. A. Tran, "Dga botnet detection using supervised learning methods," in *Proceedings of the Eighth International Symposium on Information and Communication Technology*. ACM, 2017, pp. 211–218.

[11] D. Tran, H. Mac, V. Tong, H. A. Tran, and L. G. Nguyen, "A lstm based framework for handling multiclass imbalance in dga botnet detection," *Neurocomputing*, vol. 275, pp. 2401–2413, 2018

[12] R. Sharifnya and M. Abadi, "Dfbotkiller: domain-flux botnet detection based on the history of group activities and failures in dns traffic," *Digital Investigation*, vol. 12, pp. 15–26, 2015

[13] R. A. Rodr´ıguez-G´omez, G. Maci´a-Fern´andez, and P. Garc´ıa Teodoro, "Survey and taxonomy of botnet research through life-cycle," ACM Computing Surveys (CSUR), vol. 45, no. 4, p. 45, 2013.

[14] W. Sturgeon, "Net pioneer predicts overwhelming botnet surge," ZDNet News, January, vol. 29, 2007.

[15] B. AsSadhan, J. M. Moura, D. Lapsley, C. Jones, and W. T. Strayer, "Detecting botnets using command and control traffic," in Network Computing and Applications, 2009.

[16] P. Bacher, T. Holz, M. Kotter, and G. Wicherski, "Know your enemy: Tracking botnets," 2005.

[17] H. Choi, H. Lee, and H. Kim, "Botgad: detecting botnets by capturing group activities in network traffic," in Proceedings of the Fourth International ICST Conference, ACM, 2009.

[18] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in Proceedings of the USENIX SRUTI Workshop, vol. 39, 2005, p. 44.

[19] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. ACM, 2006, pp. 41–52.

[20] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," in Emerging Security Information, Systems and Technologies, 2009. SECURWARE'. 2009, pp. 268–273.

[21] Z. Zhu, G. Lu, Y. Chen, Z. Fu, P. Roberts, and K. Han, "Botnet research survey," in Computer Software and Applications, 2008. COMPSAC'08. 32nd Annual IEEE International. IEEE, 2008, pp. 967–972.

[22] R. Villamar´ın-Salom´on and J. C. Brustoloni, "Identifying botnets using anomaly detection techniques applied to dns traffic," in Consumer Communications and Networking Conference, 2008, pp. 476–481.

[23] K.-K. R. Choo, Zombies and botnets. Australian Institute of Criminology, 2007.

[24] D. Dagon, G. Gu, C. P. Lee, and W. Lee, "A taxonomy of botnet structures," in Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual. IEEE, 2007, pp. 325–339.